登米市情報セキュリティポリシー

～　情報セキュリティ基本方針　～

平成 17 年　４月　１日　制定
令和　３年 12 月 24 日　改正
令和　４年　４月　１日　改正
令和　５年　９月　１日　改正
令和　７年　３月 13 日　改正

登米市　まちづくり推進部

目　　　次

１．目　的

本基本方針は、登米市(以下「本市」という。)が保有する情報資産の機密性、安全性及び可用性を維持するため、適切な管理を図り、個人情報等の保護の万全を期するとともに、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２．用 語 定 義

情報セキュリティポリシーにおける用語の定義は、以下のとおりとする。

（1）ネットワーク

本市の内部機関を相互に接続するための通信網、その構成機器(ハードウェア及びソフトウェア)をいう。

（2）情報システム

業務系の電子計算機(業務系におけるネットワーク、ハードウェア及びソフトウェア)及び記録媒体で構成され、処理を行う仕組みをいう。

（3）情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。

ただし、情報の重要性に鑑み、紙等の有体物に出力された情報を含むものとする。

（4）情報セキュリティ

情報資産の機密性、安全性及び可用性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（5）情報セキュリティポリシー

本市が所有する情報資産の情報セキュリティ対策について、総合的・体系的かつ具体的に取りまとめたもの。どのような情報資産をどのような脅威からどのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含め規定する。情報セキュリティ基本方針及び情報セキュリティ対策基準（以下「対策基準」という。）で構成する。

（6）情報セキュリティ基本方針

情報セキュリティ対策に関する統一的かつ基本的な方針であり、情報セキュリティ対策に対する根本的な考え方を表すもので、どのような情報資産をどのような脅威からなぜ保護しなければならないのかを明らかにし、情報セキュリティに対する取組姿勢を示すもの。

（7）情報セキュリティ対策基準

本基本方針を実行に移すための全ての情報システムに共通の情報セキュリティ対策の基準であり、本基本方針に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準、つまり本基本方針を実現するために何をやらなければいけないかを示すもの。

（8）情報セキュリティ実施手順等

情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順であり、情報セキュリティポリシーには含まれないものの、情報セキュリティ対策基準に定められた内容を具体的な情報システム又は業務においてどのような手順に従って実行し

ていくのかを示すもの。

（９）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(10) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(11) 可用性

情報にアクセスすることを認められた者が、必要な時に中断されることなく、情報にアクセスできる状態を確保することをいう。

(12) 基幹系（マイナンバー利用事務系）

個人番号利用事務（社会保障、地方税もしくは防災に関する事務）又は戸籍事務棟に関わる情報システム及びデータをいう。

(13) ＬＧＷＡＮ接続系

ＬＧＷＡＮに接続された情報システム及びその情報システムで取り扱うデータをいう。（基幹系（マイナンバー利用事務系）を除く。）。

(14) 内部情報系（インターネット接続系）

インターネットメール、ホームページ管理システム及び文書財務管理等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(15) 通信経路の分割

ＬＧＷＡＮ接続系と内部情報系（インターネット接続系）の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(16) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無いなど、安全が確保された通信をいう。

(17) 職員

本市に勤務する特別職、一般職及び会計年度任用職員のうち、市の所掌する情報資産を取り扱う者の総称をいう。

(18) 外部委託者

契約等に基づいて作業する業務委託先社員等のうち、本市の所掌する情報資産を取り扱う者の総称をいう。

３．ポリシーの位置付け

情報セキュリティポリシーは、本市が管理する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

なお、情報セキュリティ対策基準および情報セキュリティ実施手順等は公開することにより本市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

４．対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（1）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（2）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3）地震、落雷、火災等の災害によるサービス及び業務の停止等

（4）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（5）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

5．適用範囲

（1）行政機関の範囲

基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

（2）適用対象者

職員、会計年度任用職員及び外部委託者とする。

（3）情報資産の範囲

対象とする情報資産は、次のとおりとする。

① ネットワーク及び情報システム並びにこれらに関する設備及び電磁記録媒体

② ネットワーク及び情報システムで取り扱う情報（印刷した文書を含む。）

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

6．職員等の遵守義務

すべての職員、会計年度任用職員等（以下「職員等」という。）は、情報セキュリティの重要性について十分な認識を持つとともに、以下に掲げる義務を負うものとする。

ア） 本市の情報セキュリティポリシーに同意し、遵守しなければならない。また、情報セキュリティ対策を有効に機能させなければならない。

イ） 職務上知りえた秘密を漏らしてはならない。その職を退いた後も同様とする。

ウ） 委託者を使用する職員は、契約等に基づき、前述“ア)”、“イ)”と同様の内容を委託者に対しても義務付け管理する。

7．情報セキュリティ対策

情報資産の管理者及び情報システムの管理者は、本市が所掌する情報資産を脅威から保護するために、以下に掲げる情報セキュリティ対策を講ずる。

（1）組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（2）情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（3）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

① マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

② LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③ インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（4）物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷、妨害等から保護するために物理的な対策を講ずる。

（5）人的セキュリティ対策

職員及び外部委託者に対して情報セキュリティの重要性を認識させ、情報セキュリティの啓発に有効と考えられる教育及び訓練等、必要な対策を講ずる。

（6）技術的セキュリティ対策

情報システムの誤操作、不正アクセス等から適切に情報資産を保護するために、情報資産へのアクセス制御、ネットワークの管理及びコンピュータウイルス対策等の技術的な対策を講ずる。

（7）運用等におけるセキュリティ対策

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（8）業務委託と外部サービス(クラウドサービス)の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講ずる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講ずる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービス運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

(9)評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向

上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

８．情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーが遵守されていることを検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

９． 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。特に、国の情報セキュリティポリシーガイドラインの改正等があった際には、市セキュリティポリシーに与える影響が多いことから、改正内容をよく理解するとともに、原則３か月以内に改正を行う。また、組織改編等に伴う担当部署の名称変更等については適宜見直しを行う。

１０．情報セキュリティ対策基準の策定

本基本方針に従い、本市における情報セキュリティ対策の統一基準となる情報セキュリティ対策基準を定め、想定される脅威に対応するための対策要件を規定する。

１１．情報セキュリティ実施手順の策定

本基本方針及び情報セキュリティ対策基準に従い、情報セキュリティ対策に関する手法、手順の詳細となる情報セキュリティ実施手順等を策定する。